1	What is claimed is:	
2	1.	A method for a network, comprising:
3	deter	mining suspicious network activity on the network;
4	receiv	ving an initial packet from a first machine for establishing a communication
5	session bety	ween the first machine and a second machine;
6	sendi	ng a test to the first machine, the test having at least one characteristic
7 .	making the t	test resistant to automatic answering of the test; and
8	estab	lishing the communication session between the first and second machines
9	after a valid	response is received to the test.
10		,
11	2.	The method of claim 1 further comprising responding to the initial packet
12	from the firs	t machine by sending a response packet to the first machine encoding a
13,	connection	state for establishing the communication session.
14		
15	3.	The method of claim 2 wherein the initial packet is a SYN packet in accord
16	with the TCF	P protocol and the response packet is a SYN ACK packet in accord with the
17	TCP protoco	ol.
18		
19	4.	The method of claim 3, wherein the SYN ACK comprises a number
20	encoding a first address for the first machine on the network, and a second address for	
21	the second i	machine on the network.
22		
23	5.	The method of claim 2, wherein the connection state of the response

packet comprises a number encoding a first address for the first machine on the

24

1	network, a second address for the second machine on the network, and a secret	
2	unknown to the first machine to facilitate validating an acknowledgement from the first	
3	machine responsive to the response packet.	
4		
5	6. The method of claim 1, further comprising:	
6	receiving an acknowledgement packet from the first machine responsive to the	
7	response packet;	
8	decoding a tentative connection state information from the acknowledgement	
9	packet; and	
10	determining if the tentative connection state information is valid.	
11		
12	7. The method of claim 1, further comprising:	
13	preparing a web page embodying the test; and	
14	said sending the test to the first machine including sending the web page to a	
15	networking application program of the first machine, the networking application progran	
16	operative to receive and display the web page.	
17		
18	8. The method of claim 1, wherein the test is embodied within a web page.	
19 20	9. The method of claim 1, further comprising:	
21	monitoring by a monitoring device of attempts to establish communication	
22	sessions with the second machine;	
23	wherein the establishing the communication session between the first and	
24	second machines includes the monitoring device establishing a first connection between	

42390.P16364 - 19 - Patent

'	the monitoring device and the first machine, and the monitoring device establishing a		
2	second connection between the monitoring device and the second machine.		
3			
4	10. The method of claim 1, further comprising:		
5	monitoring by a monitoring device of attempts to establish communication		
6	sessions with the second machine;		
7	wherein the establishing the communication session between the first and		
8	second machines includes the monitoring device storing an identifier for the first		
9	machine in a list identifying machines that have provided the valid response.		
10			
11	11. A method for a monitoring device to facilitate communication between a		
12	client and a protected server, comprising:		
13	receiving a first packet from the client to begin a handshake for establishing a		
14	first network connection between the client and the intermediary;		
15	sending a second packet to the client to acknowledge the first packet;		
16	receiving a third packet from the client acknowledging the second packet;		
17	receiving a data access request from a networking application program of the		
18	client; and		
19	sending a test to the networking application program, the test having at least one		
20	characteristic making the test resistant to automatic answering of the test.		
21			
22	12. The method of claim 11, further comprising:		
23	receiving a response to the test from the client;		
24	determining the response comprises a valid answer to the test;		

1	establishing a second network connection between the monitoring device and the	
2	protected server; and	
3	facilitating communication between the client and the protected server.	
4		
5	13. The method of claim 11, wherein the monitoring device does not allocate	
6	resources for tracking a state information for establishing the first network connection	
7	and instead encodes the state information within the second packet.	
8		
9	14. The method of claim 11, wherein the third packet encodes a known	
10	alteration of the state information.	
11		
12	15. The method of claim 11, wherein the data access request is a GET	
13	request formatted with respect to HyperText Transport Protocol (HTTP).	
14		
15	16. The method of claim 11, wherein the networking application program	
16	includes a web browser, and the test comprises a web page incorporating the test.	
17		
18	17. A system, comprising:	
19	a protected server responsive to network connection requests;	
20	a client machine seeking to establish communication with the protected server;	
21	and	
22	a monitoring device communicatively interposed between the protected server	
23	and the client machine, wherein the monitoring device is configured to send a test	

42390.P16364 - 21 - Patent

resistant to automatic answering to the client machine, and to facilitate establishing the

24

19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: determining suspicious network activity on the network; receiving an initial packet from a first machine for establishing a communicative session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	1	client machine communication with the protected server if a valid response to the test is	
18. The system of claim 17, wherein the monitoring device is further configured to perform: receiving an initial packet from the client machine for establishing a communication session; and responding to the initial packet by sending a response packet to the client machine encoding a connection state for establishing the communication session. 10 19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: determining suspicious network activity on the network; receiving an initial packet from a first machine for establishing a communication session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	2	received by the monitoring device.	
configured to perform: receiving an initial packet from the client machine for establishing a communication session; and responding to the initial packet by sending a response packet to the client machine encoding a connection state for establishing the communication session. 10 19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: determining suspicious network activity on the network; receiving an initial packet from a first machine for establishing a communicative session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	3		
receiving an initial packet from the client machine for establishing a communication session; and responding to the initial packet by sending a response packet to the client machine encoding a connection state for establishing the communication session. 10 19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: determining suspicious network activity on the network; receiving an initial packet from a first machine for establishing a communicative session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	4	18. The system of claim 17, wherein the monitoring device is further	
responding to the initial packet by sending a response packet to the client machine encoding a connection state for establishing the communication session. 10 11 19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: 14 determining suspicious network activity on the network; 15 receiving an initial packet from a first machine for establishing a communicative session between the first machine and a second machine; 16 sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and 19 establishing the communication session between the first and second machine; 20 after a valid response is received to the test.	5	configured to perform:	
responding to the initial packet by sending a response packet to the client machine encoding a connection state for establishing the communication session. 10 19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: 14 determining suspicious network activity on the network; 15 receiving an initial packet from a first machine for establishing a communicative session between the first machine and a second machine; 16 sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and 19 establishing the communication session between the first and second machine; 20 after a valid response is received to the test.	6	receiving an initial packet from the client machine for establishing a	
machine encoding a connection state for establishing the communication session. 10 11 19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: 14 determining suspicious network activity on the network; 15 receiving an initial packet from a first machine for establishing a communication session between the first machine and a second machine; 17 sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and 19 establishing the communication session between the first and second machine; 20 after a valid response is received to the test.	7	communication session; and	
19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: determining suspicious network activity on the network; receiving an initial packet from a first machine for establishing a communicative session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	8	responding to the initial packet by sending a response packet to the client	
19. An article comprising a machine-accessible media having associated wherein the data, when accessed, results in a machine communicatively coupled network performing: 14. determining suspicious network activity on the network; 15. receiving an initial packet from a first machine for establishing a communicative session between the first machine and a second machine; 16. sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and 19. establishing the communication session between the first and second machine; 20. after a valid response is received to the test.	9	machine encoding a connection state for establishing the communication session.	
wherein the data, when accessed, results in a machine communicatively coupled network performing: determining suspicious network activity on the network; receiving an initial packet from a first machine for establishing a communication session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	10		
network performing: determining suspicious network activity on the network; receiving an initial packet from a first machine for establishing a communicate session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	11	19. An article comprising a machine-accessible media having associated data	
determining suspicious network activity on the network; receiving an initial packet from a first machine for establishing a communicate session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	12	wherein the data, when accessed, results in a machine communicatively coupled with a	
receiving an initial packet from a first machine for establishing a communication session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	13	network performing:	
session between the first machine and a second machine; sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second machine; after a valid response is received to the test.	14	determining suspicious network activity on the network;	
sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and establishing the communication session between the first and second macl after a valid response is received to the test.	15 .	receiving an initial packet from a first machine for establishing a communication	
making the test resistant to automatic answering of the test; and establishing the communication session between the first and second macl after a valid response is received to the test.	16	session between the first machine and a second machine;	
establishing the communication session between the first and second macl after a valid response is received to the test.	17	sending a test to the first machine, the test having at least one characteristic	
20 after a valid response is received to the test. 21	18	making the test resistant to automatic answering of the test; and	
21	19	establishing the communication session between the first and second machines	
	20	after a valid response is received to the test.	
		20. The article of claim 19 wherein the machine-accessible media further	

23

42390.P16364 - 22 -Patent

includes data, when accessed, results in the machine performing:

1	responding to the initial packet from the first machine by sending a response	
2	packet to the first machine encoding a connection state for establishing the	
3	communication session.	
4		
5	21. An article comprising a machine-accessible media having associated data	
6	for a monitoring device to facilitate communication between a client and a protected	
7	server, wherein the data, when accessed, results in a machine performing:	
8	receiving a first packet from the client to begin a handshake for establishing a	
9	first network connection between the client and the intermediary;	
10	sending a second packet to the client to acknowledge the first packet;	
11	receiving a third packet from the client acknowledging the second packet;	
12	receiving a data access request from a networking application program of the	
13	client; and	
14	sending a test to the networking application program, the test having at least one	
15	characteristic making the test resistant to automatic answering of the test.	
16		
17	22. The article of claim 21 wherein the machine-accessible media further	
18	includes data, when accessed, results in the machine performing:	
19	receiving a response to the test from the client;	
20	determining the response comprises a valid answer to the test;	
21	establishing a second network connection between the monitoring device and the	
22	protected server; and	

42390.P16364 - 23 - Patent

facilitating communication between the client and the protected server.

23